16TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM

"Collective C2 in Multinational Civil-Military Operations"

Command and Control Concepts and Solutions for Major Events Safety and Security: Lessons Learned from the Canadian Experience with Vancouver 2010 and G8/G20 Events

Topic 2: Approaches and Organizations

Topic 10: C2, Management, and Governance in Civil-Military Operations

Topic 1: Concepts, Theory, and Policy

POC: Adel Guitouni
Decision Support Systems Section
Defence Research and Development Canada – Valcartier
2459 Pie-XI Blvd North
Val-Bélair, Québec
G3J 1X5, Canada
Tel. (418)844-4000 ext. 4302
Email : adel.guitouni@drdc-rddc.gc.ca

Donna Wood
Project Manager
Defence Research and Development Canada – Centre for Security Science
222 Nepean St.,
Ottawa, ON, Canada
K1A 0K2
Tel: 613-943-2472
Email: donna.wood@drdc-rddc.gc.ca

Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JUN 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**
4. TITLE AND SUBTITLE **Command and Control Concepts and Solutions for Major Events Safety and Security: Lessons Learned from the Canadian Experience with Vancouver 2010 and G8/G20 Events**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence R&D Canada - Valcartier,Decision Support Systems Section,2459 Pie-XI Blvd North,Val-B?ir, Qu?c G3J 1X5, Canada,**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.

14. ABSTRACT

Planning and execution of major events safety and security operations is a very complex. Major events are often led, planned and executed jointly by many government departments and agencies in collaboration with several other actors of the civil society. Command and Control (C2) of major events can be viewed as systemic execution of collective collection, collation and analysis of information, planning, decision-making, coordination, execution and sustainment of operations and activities carried out by several agencies governed by different jurisdictions. Moreover, C2 constructs for major events spans across many domains (or pillars), each involving a set of heterogeneous and multi-jurisdictional agencies and organizations. Therefore, coordinating and integrating many stakeholders C2 operating constructs are very complex and require huge efforts, good will and important resources. Based on the empirical lessons observed from Vancouver 2010 and G8/G20 events held in Canada during 2010, it appears that cross agencies communication, coordination, collaboration and integration are key conditions for a successful C2 of major events. Shared situation awareness, common intent, trust in distributed teams, communication and information sharing strategies are key enablers for major events C2 effectiveness. In this paper, we report on major event safety and security C2 constructs and concepts. We discuss its implementation based on lessons learned from the Canadian experience.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**34**	

Command and Control Concepts and Solutions for Major Events Safety and Security: Lessons Learned from the Canadian Experience with Vancouver 2010 and G8/G20 events

Abstract: Planning and execution of major events safety and security operations is a very complex. Major events are often led, planned and executed jointly by many government departments and agencies in collaboration with several other actors of the civil society. Command and Control (C2) of major events can be viewed as systemic execution of collective collection, collation and analysis of information, planning, decision-making, coordination, execution and sustainment of operations and activities carried out by several agencies governed by different jurisdictions. Moreover, C2 constructs for major events spans across many domains (or pillars), each involving a set of heterogeneous and multi-jurisdictional agencies and organizations. Therefore, coordinating and integrating many stakeholders C2 operating constructs are very complex and require huge efforts, good will and important resources. Based on the empirical lessons observed from Vancouver 2010 and G8/G20 events held in Canada during 2010, it appears that cross agencies communication, coordination, collaboration and integration are key conditions for a successful C2 of major events. Shared situation awareness, common intent, trust in distributed teams, communication and information sharing strategies are key enablers for major events C2 effectiveness. In this paper, we report on major event safety and security C2 constructs and concepts. We discuss its implementation based on lessons learned from the Canadian experience.

1   Introduction

Major events are often co-sponsored, planned and executed jointly by public and private-sector interests across multiple government jurisdictions. Major events topics include competitive amateur sport events, cultural, political, economic, health or environmental and social just to name a few. In 2010, Canada was the host for several major events like the Vancouver 2010 Olympics and Paralympics games (V2010), G8 and G20 meetings.

The Defence R&D Canada (DRDC) was involved with V2010 preparedness since 2005. Initially, DRDC's effort was packaged within an experimental campaign plan in support of the Department of National Defence (DND), Canadian Forces Experimentation Centre (CFEC), Canada Command (CanadaCOM) and the Royal Canadian Mounted Police (RCMP). This activity served as a central coordination point for various S&T activities. Joint Command Decision Support for the 21st Century Technology Demonstration (JCDS21 TD) is an example of the type of S&T effort that was leveraged in support of V2010. In 2007, a full scale Command and Control experiment called PEGASUS GUARDIAN 1 (PG1) was held in British Columbia and served to unite many of the S&T activities, as well as key players responsible for V2010 security planning. This work allowed V2010 Integrated Security Unit (ISU) to develop and test its initial processes under controlled conditions. The parallel work of CFEC and JCDS21 experiments at PG1 provided an early opportunity for S&T support to a major event like the V2010. A full scale project has then been stood up by the Chief Executive Officer (CEO) of DRDC to take ownership of the ongoing activities in support of the ISU and the Joint Task Force Games (JTFG). The Project then set out to develop a delivery model that would build on existing work and relationships within the security partnerships, and facilitate the opportunity for S&T contributions. The Project was named Major Events Coordinated Security Solutions (MECSS).

The MECSS Project is a multi-agency collaborative S&T partnership, established to reduce the security risk associated with V2010 and the G8/20 events. MECSS was implemented as a formal project within the Public Security Technical Program, under DRDC management through the Centre for Security Science (CSS). The objectives of the MECSS project were to:

a. Assist the functional authorities in reducing the security risk associated with V2010 and the G8/20 through the coordinated application of science and technology, and

b. Contribute to the establishment of an enduring Major Event security architecture that can be applied to future Major Events in Canada.

In this paper, we focus on the Command and Control aspect of Major Events. These events are governed by a complex framework of laws, legislations and inter-governmental agreements that most often mandates that the RCMP acts as the lead agency for the planning and execution of major events safety and security operations in Canada—particularly for those major events safety and security operations that affect national interests or national security, or require federal leadership, coordination and funding.

The remaining of this paper is organized as follows. In section 2, we discuss the complexity of major events. In section 3, we present different contributions of the S&T community to the Command and Control solutions for major events. In section 4, we present a major event C2 framework. In section 5, we discuss best practices and the prerogatives of major events C2 solutions. In section 6, we present the conclusion.

2 Complexity of the Command and Control arrangements for Major Events

Complexity can be defined as the composition and interaction of variables in a situation that affects the sources and accuracy of information, the communication and decision-making processes, and the nature of activities that are required in order to arrive at a desired end-state. Complex situations involving asymmetric threats require a collaborative response from a variety of stakeholders. It is characterized by a number of factors such as: time sensitive response activities, simultaneous life-threatening incidents across multiple geographic locations, multi-stakeholder interaction that require collaboration of numerous organizational cultures to facilitate personnel and equipment resource sharing, information feeds and communication channels that include computer, phone and liaison officer interaction, informal and formal processes, and the constraints of policy and legal issues, to name a few. The character of V2010 causes interdependencies and workflows in the areas of collaboration and decision making to be tested and challenged at all levels (JCDS TD, 2008).

The V2010 Integrated Security Unit construct has a number of key influences that impact the articulation of stakeholders' relationships, command and control and decision-making capabilities. Domestic incident response environments are framed by a hierarchy of relationships that are defined by legislation, policy, public security and emergency response plans[1]. Domestic incident response environment are framed by a hierarchy of relationships that are defined by legislation, policy and emergency response plans[2]. These facilitate the ability for multiple governments, departments and agencies across Canada to share resources and provide a mechanism for interagency collaboration. Canadian domestic legislation, such as the National Defence Act and the Emergencies Act, and policy, such as the National Security Policy, provide

---

[1] More detail on the processes involved in Canadian emergency response can be found in *Emergency Response in Canada: A Review of Procedures and a Generic Collective Response Model*.

[2] More detail on the processes involved in Canadian emergency response can be found in *Emergency Response in Canada: A Review of Procedures and a Generic Collective Response Model*.

guidance for emergency response plans at the federal, provincial and municipal levels. Provincial and municipal legislation, i.e., Emergency Acts, follow the lead set by the federal or provincial level. Federal emergency response plans such as the National Support Plan, the National Counter-Terrorism Plan, and the Federal Nuclear Emergency Response Plan, form a hierarchy that guide and are supported by federal government agency plans (such as the Canadian Forces doctrine for the Conduct of Domestic Operations (DDDO) and Health Canada's National Smallpox Contingency Plan), as well as provincial and municipal government emergency response plans and their associated agencies and departments. Continentally, documents such as the Joint Canada-US Radiological Emergency Plans are also written within the framework of the federal plans, and provide a mechanism for collaboration with the US.

Command and Control is fundamentally a human activity. Organization and technology exist to support the human dimension of decision-making. In essence, the C2 of major events can be viewed as systemic execution of collective collection, collation and analysis of information, planning, decision-making, coordination, execution and sustainment of operations and activities. C2 of V2010 was multi-layered and spanned across at least three domains (pillars), each involving a set of heterogeneous and multi-jurisdictional agencies and organizations as shown in Figure 1.
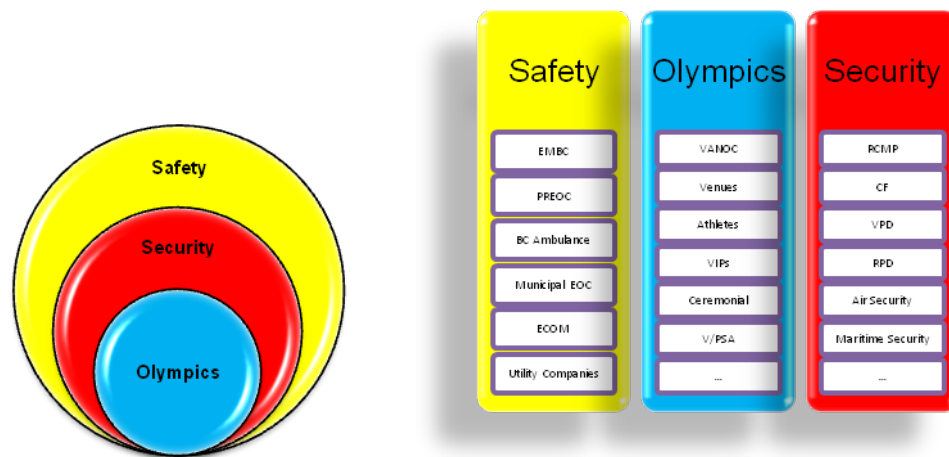

Figure 1: (A) Multi-Layered Operations: (B) Three Pillars with Multi-Stakeholders

V2010 C2 arrangements are not unique in the Canadian context. Figure 2 illustrates the main functions of an Incident Command System (ICS). Although there is no formal, standardised structure for Canadian government agencies or departments, many civilian organisations have applied the ICS framework. For example, the province of British Columbia (BC) has adopted the framework for organizing emergency management activities at all levels. In BC, the provincial regional coordination level acts in support of the site support level, and manages the assignment of multiple-ministry and agency support to individual site support locations or multiple site support level locations, acquires and deploys resources at the request of the site support level, and provides emergency response services where incidents cross local authority boundaries, or where local authorities may not have the infrastructure to fulfil their role.

Major Events Command and Control constructs revealed a number of common variables with emergency situations resulting from terrorist activities and asymmetric threats. Many variables have been identified into an overall framework that can characterize Complex Situations. This framework introduces four broad categories of variables that influence the complexity of a response situation (see Figure 3):
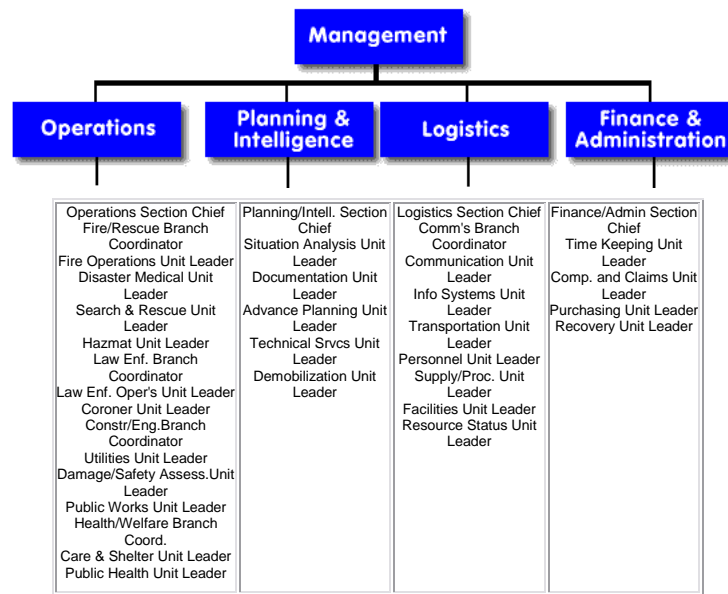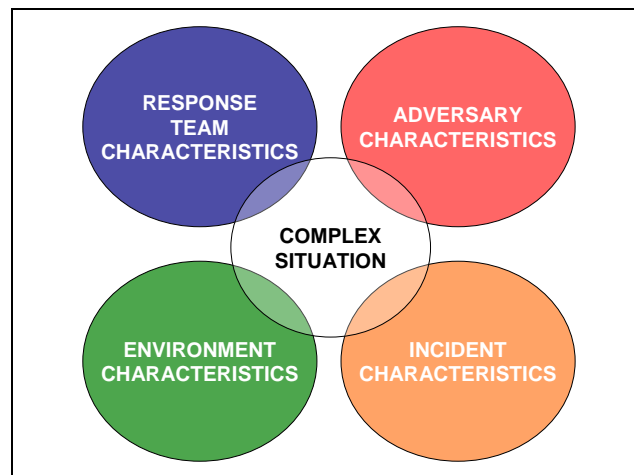
Figure 2: Incident Command System Structure[3]

Figure 3: Categories of Variables that Influence the Complexity of Response Situations

- Response Team Characteristics: The composition, characteristics, and behavioural norms of the Response Team influence the complexity of the situation. Variables in this category include: Number of Participants, Number of National Actors, Number of Agencies, Number of Different Types of Agencies, Complexity of Organizational Structure, Stability of Organizational Structure, Organizational Procedures (the "chain of command"), Number of Communication Channels (n(n-1), Level of Interoperability, Level of Preparedness for Attack…

- Adversary Characteristics: The composition, characteristics, and behavioural norms of the Response Team influence the complexity of the situation. Variables in this category include: Number of

---

[3] Federal Emergency Management Association (USA) website http://www.fema.gov/, accessed May – October 2004.

Participants, Number of National Actors, Number of Agencies, Number of Different Types of Agencies, Complexity of Organizational Structure, Stability of Organizational Structure, Organizational Procedures (the "chain of command"), Number of Communication Channels (n(n-1)), Level of Interoperability, Level of Preparedness for Attack…

- Environment Characteristics: The composition, characteristics, and behavioural norms of the adversary influence the complexity of the situation. In situations where there is an adversary (such as asymmetric threat and terrorism) the variables in this category include: Degree of Financial Support, Speed of Adversary Decision Cycle, Level of Violence, Level of Asymmetry in Adversary Organization, Level of Asymmetry in Adversary Tactics, Level of Threat Visibility…

- Incident Characteristics: The characteristics of the attack or incident influence the complexity of the situation. Variables in this category include: Level of Attack Surprise, Breadth of Incident, Number of Causalities, Level of Public/Responder Fear, Level of Restraint Required, Level of Fluctuation Between Action and Restraint, Level of Time Pressure, Number of Possible Response Contingencies, Level of Novel Problem Solving Required to Plan Response, Long Term vs. Short Term Effects of Incident (Overt vs. Covert)…

The results of the analysis conducted to understand the Canadian incident response environment and emergency response scenarios for this project enabled the development of a Generic Collective Response Model (GCRM) model of the collective response to emergencies caused by terrorist attacks and other asymmetric threat situations. Example of response patterns that were identified during the literature review, such as response activation, formed the base structure for the GCRM (see figure 4). In addition, the need to recognize the elements of organizational complexity was considered as shown in figure 5.
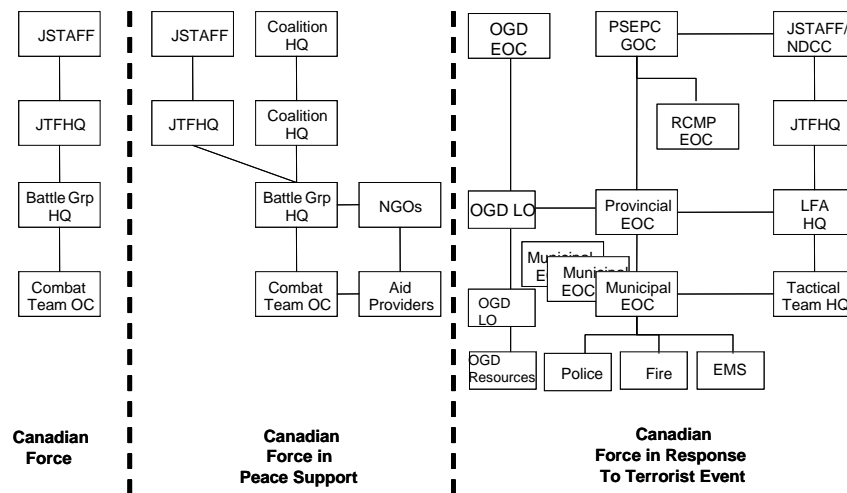

Figure 4: General Response Activation Pattern

Figure 5: Example of Increasing Organizational Complexity

Therefore, examining the best options for command and control, organisational integration, and best practices for sharing information, standard operating procedure (SOPs) and response plans have been investigated through formal studies and an exercise campaign to influence the structuring of the ISU and its Integrated Command Center (ICC), as well as the Command and Control structure of the Joint Task Force Games (JTFG) in support of the ISU.

Therefore, it is not surprising that the C2 has been the main integration layer for V2010 operations. V2010 C2 involved many organizations, command and operations centers scattered throughout the Vancouver and Whistler regions. Moreover, many other existing command and emergency management centers have been integrated in this C2 concept of operations. Coordination and integration of many agencies and stakeholders involved huge enterprise coordination and management effort. Key coordination effort includes determining objectives, establishing the appropriate competence, authority and responsibility constructs, and allocating resources. Direction has become synonymous with Common Intent. Cohesion and inclusion of different agencies and stakeholders have become important enablers and unified direction for success. Therefore, C2 of major events is a very dynamic domain. Communication, coordination, collaboration and integration have been considered key enablers for a successful C2 solution. Shared situation awareness, common intent, trust in distributed teams, communication and information strategies are key foundations for major events C2 effectiveness. Consequently, maintaining a common knowledge base and sustaining trust among heterogeneous stakeholders and organizations has been the main C2 challenge during V2010.

3   C2 Relared S&T Contributions through MECCS

MECSS C2 contributed to maturing the C2 concepts and constructs of V2010 ISU. Many lessons learned and expertises developed during V2010 have then been exploited in support of the ISU for the G8/G20. MECSS C2 team has been involved with many C2 related activities (Wood et al., 2010). The different agencies that benefited from S&T support in preparation of V2010 and G8/G20 include, but not limited to, JTFG, ISU V2010, ISU G8/G20, Privy Council Office (PCO), OMOC, RCMP National Operations Centre, CBRNE National Team, and British Columbia Integrated Public Safety (BC IPS). We describe some of these activities in remaining of this section.

ISU C2 CONOPS: MECSS C2 team made significant contributions to the development of the ISU C2 concept of operations (CONOPs) by conducting a quick set of stakeholder interviews and drafting of the

initial narrative for the ISU C2 CONOPs. The deliverables have then been integrated into the final ISU C2 CONOPs.

Command Centre Design: This activity involved science and technology (S&T) support for performing ergonomic analysis and workspace design for ISU operations and command centres throughout the area of operation. A series of studies have been conducted in which workspace solutions were produced for Theatre Command Centre, Vancouver Area Command Centre, Whistler Area Command Centre, Air Support Operations Command Centre, Olympic Marine Operations Centre and CF Games Joint Operations Centre. In these studies, an Alternative method for Workspace Analysis and Design (AWAND) was proposed and then further developed and used to design and implement novel Command Post layout. For example, MECSS introduced a new Command Post layout based on the notion of pods regrouping staff positions with potential for high interaction and collaboration or based on functional specialties. Disposition of the different pods in the command centers is based on cross pods information exchange and collaboration requirements to facilitate seamless information flows and foster cross functional collaboration.

V2010 C2 Architecture and Process Modeling: This activity provided analysis support to help the ISU and its security partners to build a viable C2 architecture. This work helped to identify functional goals, articulate the aligned operational processes and determine the IM/IT systems needed to support them. The work leveraged the knowledge gained from Exercise Pegasus Guardian and prior work modeling C2 Architecture for other segments of the CF.

Collaboration Framework: This work was done to support the ISU and exploited previous DRDC work in order to provide advice as to how the various organizations involved in domestic security during the 2010 Olympics might optimize their collaboration in order to maximize operational effectiveness. Moreover, MECSS leveraged the database of more than 400 questions to evaluate collaboration during different V2010 Exercises.

Confirmation Architecture Framework (CONAF): CONAF was initiated to support V2010 ISU C2 confirmation, by providing functional groups with a framework for developing a set of criteria used during the final exercises to confirm their state of readiness/preparedness for V2010. The CONAF structure articulated what the process is, how it relates to the business and who needs to be a part of the process. During each exercise, a team of scientists have been deployed in each command center to collect data according the different assessment criteria. Each day, all observations and metrics were compiled and discussed by the team and merged into an aggregated evaluation matrix. The cumulative result for each day and for the exercise have used by the staff to discuss different issues related to the Command and Control constructs. The discussions also facilitated bringing together groups who had never met to talk about processes linking them.

IT Architecture Options Analysis: This work involved consulting with a number of experts in network design and providing some input on the impact of selecting a thin versus thick client network architecture for the ISU. A multiple criteria decision analysis method has been used to evaluate different options based on the different stakeholders and subject matter experts' inputs.

Communication and Information System (CIS) Studies: MECSS C2 team conducted several studies in support of the deployment of the Communication and Information Systems planning (e.g., JTFG V2010 CIS). This work was guided by the following considerations:

- Accessibility of C2 application deployment in support of the V2010 C2 concept of operation and the Commander and its staff information exchange requirements,

- Enforcing information protection and security prerogatives while satisfying information sharing requirements with other agencies and information flows between the different level of command,

- Development and enforcement of different mitigation strategies for potential vulnerabilities,

- Design, implementation and sustainment of CIS infrastructure,

- Crypto support (tactical thru Strategic),

- User-Helpdesk-Consolidated Support Desk integration, synchronization and harmonization, and

- Operational plenary, prioritization, command, coordination, consultation processes and interagency integration protocols.

Scientific and technical team have been tasked by auditing the CF CIS architecture and solutions deployed in support of V2010. The team conducted a detailed survey, documented and analysed the deployed CF CIS architecture across the Joint Area of Operation. A set of interactive map-based documentation were delivered to JTFG and deployed on Command Net to support planning, trouble shooting and redeployment of JTFG CIS infrastructure. These results were also used to provide the Commander of JTFG with an assessment of the CIS OP Readiness.

MECSS C2 team investigated, designed and contributed to the deployment of an information sharing solution on Command Network. This solution was based on Microsoft SharePoint. The team designed and implement a CIS dashboard which was used for daily commander's briefs. The SharePoint solution is a legacy that was transitioned to JTFP.

Deployment of C4ISR Mobile Lab: DRDC C4ISR mobile lab was transferred to Joint Task Force Games for deployment in support of V2010. The C4ISR mobile lab is a 53 feet trailer equipped to host C4ISR tasks and teams up to Top Secret. The lab is autonomous and mobile. JTFG made significant upgrades and installed several additional C4ISR systems used during different exercises and during the operation. DRDC scientists contributed to upgrading, employing and redeploying of the C4ISR Lab.

Olympic Maritime Operation Center Analysis: MECSS C2 team provided operational analysis support to the Olympic Maritime Operation Center (OMOC), primarily through the application of a methodology for conducting a table top exercise, known as the Australian Force Protection Matrix Game. This activity was well received by the OMOC which led to the delivery of three Force Protection Matrix Games.

Shift Scheduling and Mobilization Planning: This activity was initiated to develop optimization model and application for work force scheduling at various distinct locations. The proposed model took into account the varying staffing levels required throughout each day at each location. The model was flexible enough to allow for changes in the staffing levels, and assists in planning in cases of surge requirements. The model was developed based on mathematical optimization formulation and used Ilog CPlex solver.

Scientific Support to C2 related Exercises and Experimentation: Over the period of planning for the Vancouver Olympics, DRDC supported a number of exercises ranging from table tops to command post exercises to live exercises. Different teams of scientists have been embedded with Command Centers during the different exercises and experiment. The S&T community was called upon to perform tasks including design of data collection plans, data collection, analysis and reporting. In most cases, scientific deliverables in form of letter reports were delivered to the command staff within two weeks. In some

instance, a quick feedback was documented and delivered the same day. S&T support to exercises and experimentation included deploying maturing capabilities.

4   Major Events C2 Framework

I their work for DRDC, Purian et al. (2009) proposed a major event framework based on the integration between outcome management, governance management and program management (Figure 6). The authors suggested that a major event should be seen as an enterprise delivering desired outcomes (or desired effects). Outcomes and effects should be defined as "*a measurable change, caused by the output of effort (i.e. services, processes, projects and systems) that is responsive to the recognized needs of all program beneficiaries and to the shared priorities of partners and stakeholders*" (Purian et al., 2009). Governance management defines the legal, doctrinal and agreeable arrangements between different organizations and agencies to deliver the outcomes. Purian et al. (2009) suggested that "*desired outcomes [effects] that must drive, define and confine the decision-making and the executive accountabilities that are to take place under a collaborative governance management*". The execution is therefore the implementation of an instantiated solution to deliver the outcomes under the proposed governance arrangements.

Purian et al. (2009) proposed the strategic management framework (SMF) shown in Figure 7. This framework is based on the development a clear and rich understanding of the desired outcomes of the major event itself: "*It is a step based upon the recognition that major events safety and security operations are merely the means by which stakeholders assure safe and secure accomplishment of overarching major-event ends*" (Purian et a., 2009). This framework recognizes the following critical components:

- Strategic Management includes outcome and governance management.

- Program Management includes but not limited to Lead Agency Direct Operations Management, External Support Operations Management, Human Resource Management (HRM).

- Administrative Support includes but not limited to sharing resources, information and knowledge management, corporate services.

- Major Event Safety and Security Impact Assessment which relates to continual effects assessment.

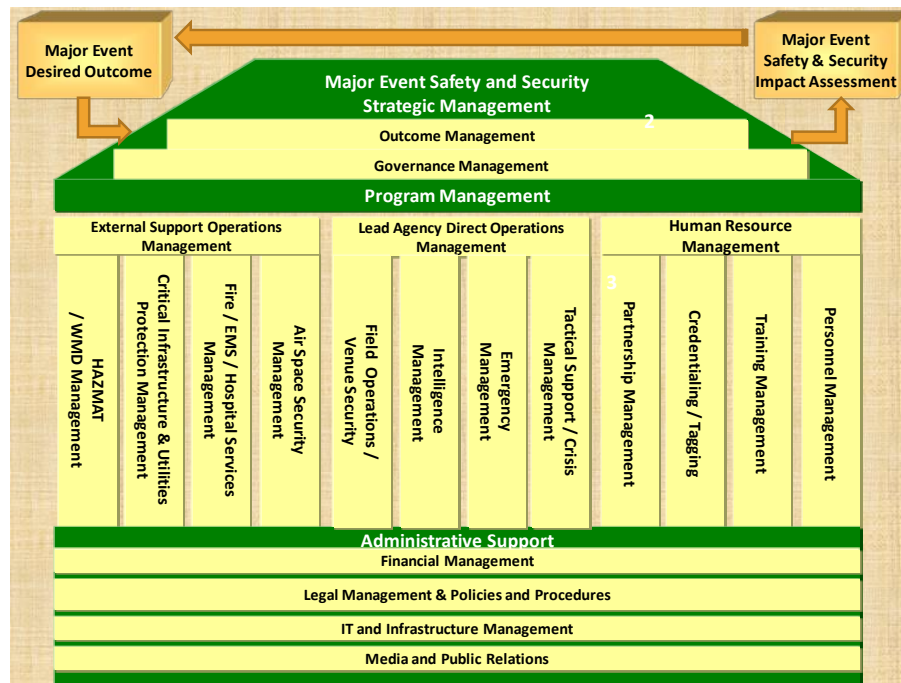Figure 6: Blending Outcome Management, Governance Management and Program Management

Figure 7: Proposed Major Events Safety and Security Framework

5   Toward Best Practices for Major Events C2 Solutions

The experience with V2010, G8 and the G20 has illustrated opportunities and challenges of cross agencies and government jurisdictions Command and Control for safety and security operations. Challenges associated with integrated planning, decision-making, execution management, communications and interoperability can be attributed to dissimilar organizational cultures, doctrines, mandates and -in many cases- to legislative constraints. The existing challenges are compounded by a national safety and security infrastructure that is challenged to fully exploit collective learning opportunities between agencies and across jurisdictions. MECSS undertook the development of Major Events Security Framework that is intended to serve for future major events planning and execution (Wood et al., 2010).

Major events go through three distinct phases: i) Planning (prior), ii) Execution (during), and Evaluation (after). There are many lessons observed from V2010, G8 and G20 events. These lessons confirm what has been observed in many other events organized by other countries like the US. For instance, US authorities from recent Olympic Games [4] reflected on the following lessons learned (Pourian et al., 2009):

- Earliest possible pre-event planning and preparation;

- Unified command and centralized security operations;

- Clearest possible articulation of titles, mandates, roles, responsibilities and accountabilities;

- Adequate and dedicated funding;

---

[4] United States Government Accountability Office, Report on Olympic Security, June 30, 2006

- Development of a generic major event safety and security operations planning framework.

Purian et al. (2009) suggested that "*A nation-wide study of major events safety and security operations conducted by the US Department of Justice[5] recently concluded that in planning and managing major events, [security officials] must:*

- *Plan for worst-case scenarios—extraordinary crimes, violence by protestors, a possible terrorist attack, natural disasters—but also be prepared to deal with ordinary crimes and incidents;*

- *Weigh strict security measures (e.g. street closures, searches, highly visible tactical units) against [stakeholder desire to deliver] events that are enjoyable, well attended and profitable;*

- *Ensure that events continue safely and at the same time respect [civil] rights;*

- *Establish innovative and effective—but temporary—organizational arrangements, management structures and methods of communication;*

- *Ensure that the rest of the [citizen] jurisdiction receives essential [safety and security services], regardless of the size or importance of the event;*

- *Ensure that appropriate federal officials…are informed in advance about events with national or international significance to guarantee federal awareness and possible support.*

The same study stressed that it "cannot be overstated…that timely, effective planning, communication and training are critical.""

In the remaining of this section we discuss the best practices for multi-agencies collaboration, planning and execution of C2 for major events. We also discuss obstacles and potential enablers based on MECSS experience.

5.1   Fostering Multi-agency Collaborations

Lead Agency: Assigning a lead agency is critical necessary but not sufficient condition for a collaborative major event management framework. Lead agency should work with other agencies and departments toward developing flexible, effective and responsive event frameworks that balance skills and resources to achieve common goals and outcomes. Lead agency can develop common rules of engagement for supporting agencies and focus their resources on maximizing team building and clarifying member roles.

Clarify Legal Authorities: It is important to develop a clear and succinct legal authorities and responsibilities. The web of legislations and regulations contributes to the fog of management and too many conflicts.

Perform Collaboration Situation Assessments: Understand the goal and the outcomes as well as the operating environment in which the major event will be held are paramount to developing shared situation awareness and understanding of the situation. Moreover, red teaming and similar challenging functions should be considered in order to help the different safety and security partners to develop a broader understanding of the threats, vulnerabilities and opportunities available to them.

---

[5] US Department of Justice Office of Community Oriented Policing Services (COPS), Major Events Security Guidelines

5.2   Collective Planning and Execution of Operations for Major Event Security

Pre-Event Planning: Planning for major events should begin as early as possible or contingency plans should be developed for unforeseen major events (e.g., non forecasted nations' leaders meeting). Planning should start with clear articulation of the expected outcomes and effects. A unique and clear governance structure should be well established. An executive planning team should then be established from capable and expert planners representing the core leading and supporting agencies and departments. It must identify other agencies including law enforcement, fire, and EMS that should be part of securing the major event. It should also enumerate each of the functional areas and responsibilities into a Command and Control framework (Bellavita, 2003). Continual planning should be adopted supported by review, collective exercises and assessment events. Plans and contingency plans should be flexible enough to update as conditions often change in the midst of the planning stage.

Organizational Framework: Major event safety and security is usually carried out by ad hoc bodies created for the event. In the case of V2010, safety operations were led by a permanent provincial emergency management body, security operations were led by an ad hoc ISU, and the Games operations by the Vancouver Olympics Committee (VANOC). Developing a draft command and control construct and a draft concept of operations are critical building blocks toward maturing an organizational framework for major event command and control solution. The purpose of an organizational framework is to make sure that all key responsibility areas are assigned and all lines of communication between agencies are identified. The following major event's key responsibility areas are:

Leadership Structure: Define which agency or department has legal and leadership authority to control the security and the safety of the event. The lead agency must also define what role will be assigned to the supporting and other agencies. Having one agency in charge of the legal and financial responsibilities of the event is crucial. Mandate clarity, roles and responsibilities of each agency are paramount for major events success.

Command and Control Centers and Infrastructures: On scene Command and Control, Communication and Coordination centers are critical enablers for major events safety and security. A central command system or a set of interoperable command systems are an efficient enablers for controlling the entire operation under one roof. A common training program involves the following management characteristics for effective, efficient, and collaborative incident management (FEMA, 2008): i) Common Terminology, ii) Reliance on an incident action plan, iii) Manageable span of control, iv) Integrated Communications, v) Unified Command, vi) Chain of Command, vii) Information and intelligence management, and viii) Pre-designated mobilization centers. The National Incident Management System (NIMS) stresses the use of plain language as a matter of public safety (FEMA, 2006 and 2008).

Assessment Model: Assessment and continual preparedness should be carried out on regular basis when all of the agencies have been brought together, and understand and accept their role in securing and safeguarding the major event. Assessment should help these agencies understand the operating environment (actors, stakeholders, threats, opportunities, potential consequences, etc.). Formal communication and continual collective exercising and self critiquing will inform plan improvement and development of contingency plans as required. Purian et al. (2009) stated that "*if the threat levels can be assessed accurately, the model can act as a cost controller because the organizing committee can enumerate the staff, equipment, training, and other costs that correspond to that threat response.*" Although it is impossible to determine and enumerate all possible threats due to the uncertainty and unpredictability of future occurrences the risk assessment model is one that has been used successfully in most of the past major events (Johnson, 2006).

Collective and Individual Training: Training for major events often takes a progressive approach evolving from classroom sessions, to tabletop exercises, command post exercises and finally to field training exercises. Privy Counsel Office mandated different common training and assessment events for V2010 and G8/G20 involving most of the agencies and the departments engaged with safety and security operations. This approach has shown to be very beneficial and effective bridging the different gaps among the different partners. The novelty introduced by DRDC is the employment of the S&T community to observe, collect data and produce assessment reports based on rigorous scientific approach and metrics. In some cases, scientists were instrumental to challenge the staff and expose vulnerabilities and weaknesses. Training and exercising is usually broken down into subgroups. The Salt Lake City Games in Utah organized training into (Conners, 2004): Strategic, operational, specialty, field, venue-specific Training, product/equipment/system training, etc.

Communication: Communications for a major event span almost every aspect including human resources, interagency communication, communication interoperability, and integrated command centers. In 2003, Calgary, Alberta hosted the 2003 World Trade Organization Summit. Calgary Mayor, Dave Bronconnier said: "*...the Calgary officials most attributed their success to the quality of their communication plan. That plan focused heavily on perfecting their communications and dialogue with all staff and partnering agencies, externally with the general public, and perhaps most importantly with the leaders and members of identifiable protest groups*." (Bellavita, 2003). Purian et al. (2009) stated that "*it is clearly important that security planners for major events create policies and procedures for all partners, governing officials, private security, and others to communicate regularly on major event planning and management*." During V2010, G8 and G20 several communication networks and systems have been established to support communication across different agencies. Despite all the training and the technologies deployed, seamless communication and ubiquitous information sharing continued to be a challenge.

In-Progress Reviews: Multi-jurisdictional and multi-agency collaboration requires much training and practice in order to get the different agencies working successfully in unison. In progress reviews are very valuable in keeping all groups focused, in synch, and communicating with each other (Conners, 2004).

Partnership Management: Major events related literature suggest the following common themes: clarify of the legal authority of the assisting agency, enumerate the commitment of the assisting agencies, clarify the assisting agencies duties, and compensate for the economic costs of having those agencies as a part of the security organization. It is also important to make a clear distinction between the duties of the assisting agencies and those of the lead agency.

Intelligence: Intelligence functions are usually broken down into two stages: before and during a major event. In the context of V2010, a joint intelligence group was established to become a single hub for all intelligence information sharing. This model seems to have achieved its goals despite many issues.

C2 of CBRNE Operations: Possible threats include explosives, chemicals, biological, and radiological attacks. Planning, managing and deploying CBRNE units required multi-agencies collaboration under the leadership of PCO. Up to V2010, C2 of CBRNE was lacking clarity and coordination. A new concept of operations was developed and validated through many exercises and then during the execution phase. Moreover, on an experimental basis scientific capabilities have been deployed to the area of operations. These capabilities were clustered into two science towns in Vancouver and Whistler to support the national team. Placement of risk assessment teams and sensing capabilities inside and around of venues has become standard procedure for major special events.

Public Safety – Fire, EMS and Public Health-: V2010 safety operation was led by a distinct body called the Integrated Public Safety (IPS). In Canada, public safety is a provincial jurisdiction. Thus, Emergency Management BC led IPS and coordinated Fire, EMS, and Public Health to protecting the safety of the public during V2010. This model seemed to be efficient. C2 of IPS and its relationships with ISU and VANOC has been assessed through different events with DRDC scientific support. Embedding a scientist with IPS appears to have been an excellent move that brought benefits to IPS, ISU and Canadian Forces.

Public Affairs: V2010 involved communication of information to partner agencies, governments, spectators, athletes, businesses, community members, and the media. V2010 Safety and Security Public Affairs were managed by an integrated public affairs unit with representatives from all key agencies. This unit developed and implemented a coordinated public information and media relations plan co-located with the Integrated Security Unit. This model seems to have been efficient. This unit has been established early in the process and participated in all training and exercising events.

Private Sector Coordination: Many critical services and infrastructures are owned and delivered by the private sector (e.g., utility, communication). Many private sector enterprises have been engaged and involved throughout the different phases of V2010. It has been a positive and constructive experience for all partners. Moreover, many private security personnel often assisted with access control, screening transport vehicles, or monitoring the inner-perimeter of venues.

5.3   Potential Obstacles

Many factors contribute to a limited and ineffective collaboration. In this section, we discuss some these obstacles observed in different exercises and training events.

Limited Information Sharing: For many reasons, information sharing might be limited (e.g., security clearance, technology, human). However, poor information sharing is a prominent and ongoing issue in multi-agency collaborations. Purian et al. (2009) suggested that "*in many cases, information sharing between agencies is complicated by statutes such as privacy acts, which limit how, when, and with whom essential information and data is shared. To make matters worse, agencies often interpret the provisions of these acts differently when planning for and responding to major events, which can lead to inconsistent policy formulation and high tensions. Information sharing can also be limited if non-standardized communications, data storage and knowledge management technologies are used across coordinating organizations. These varying technologies often create compatibility issues and can lead to a hesitation amongst agencies to cooperate (Management Advisory Committee, 2004).*"

Interoperability Issues: Another constant collaborative challenge is the lack of interoperability between information technologies devised for multi-agency major event management. Technological interoperability can be broken down into three main elements. 1) The technical compatibility of message formats, 2) The semantic terminology and definitions used, and 3) The organizational practices and procedures implemented (Sotoodeh, 2007). Moreover, interoperability issues might also be observed at the organizational and processes level.

Lack of Common Terminology: It has been observed that a lack of common terminology across agencies within collaborative structures is a root cause of poor information sharing. Civilian and military agencies often use unique terms and acronyms to describe similar concepts and ideas as part of their internal communications structures. These kinds of communication issues often deter collaborating agencies from establishing healthy working relationships.

<u>Structural Silos</u>: Different agencies and department functioning under different governance structures, and with diverse policies and legislation, limit their cooperation and information sharing with each other due to a lack of trust, respect, or cultural understanding. This effect has been closely linked to security and law enforcement culture, where personnel are trained to be suspicious of other agencies, creating a general sense of apprehension and an overall lack of trust (Management Advisory Committee, 2004).

<u>Financial and time constraints</u>: It is too costly, in terms of time and money, to incorporate all of the best practices from past major events into the current event. Kumar (2005-2006) suggested that "*many studies have been done to identify the factors that impede knowledge sharing. For example, lack of trust, lack of time, lack of motivation, status of the knower, quality and speed of transfer all contribute as obstacles to knowledge sharing.*" All of these best practices and lessons are very valuable. However, we observed that not all were implemented during V2010 because it becomes too difficult and too costly to implement all of them into a security plan.

<u>Cultural barriers</u>: Cultural and organizational barriers exist between different agencies and departments. Purian et al. (2009) suggested that "*agencies do not use common terminology, their training teaches them how to accomplish tasks within their agency alone, and there is no training in place to build trust and relationships between agencies.*"

<u>Governance issues</u>: Lacking a clear and legitimate governance structure creates chaotic situation and confusion among different partners. Sometimes it is important to clearly mandate agencies to collaborate and provide clear provisions of resources and accountability measures. Thought, therefore there is actually a need to minimize the resistance through a greater reliance on influence, negotiation, and consensus building (Kernaghan, 2009).

5.4   <u>Potential Enablers</u>

<u>Integrated Command Structures</u>: Integrated command structures (like the ISU) allow agencies with different legal, geographical, and functional responsibilities to coordinate, plan and interact more effectively. Purian et al. (2009) suggested that agencies working under a unified command structure can overcome much of the inefficiency and duplication of effort that can occur when agencies operating within different jurisdictions, and at different levels of government, fail to share common communications systems and organizational frameworks. However, we observed that personalities (especially of the commanding officer) might have huge impact on the collaboration effectiveness.

<u>Common Information Sharing Systems and Protocols</u>: ISU put in place an emergency management system available to all agencies involved in the security of V2010 and G8/G20 events. It has been observed that information and communications technology (ICT) underpins and enables improved information sharing and information management techniques by agencies. No amount of goodwill and good policy direction is enough unless you have accurate information at your disposal. As the need for multi-agency security partnerships grows, organizations are focusing more heavily on developing information exchange and data management standards and protocols (Purian et al., 2009).

<u>Outcome Management and Cost Reduction</u>: Purian et al. (2009) suggested that outcome driven agency involvement is a practical and minimalist approach to multi-agency collaborations. Some research suggests that reducing the number of agencies involved and integrating their related functions into larger portfolios can help integrate policy, program and service delivery across agencies. The observations of V2010 suggest that coordinating agencies should focus on creating efficiency protocols and utilizing shared technologies to streamline processes and communication lines to avoid key intelligence-sharing break downs prior to major events in the future.

Scalable Governance Structures: V2010 observations and major events related literature suggest that collaborative major event governance structures should be tailored to suit the mandates and strategic objectives of all agencies involved, and should be designed for effectiveness, and to support the stakeholder roles and responsibilities. Liquid and scalable governance structures allow agencies to jump on and off board with relative ease and at minimal cost (Purian et al., 2009). Research suggests that the most successful collaborative governance models are those that are flexible, adaptable, easy to understand, and offer positive value propositions that are continually reinforced. They should also present clear, common visions that can gain and sustain stakeholder confidence (Kernaghan, 2009).

Community of interests: It is important to establish community of interests and participate in international conferences held after most major events. These conferences are usually intended to review the best practices and lessons learned from that event. Bellavita (2003) suggested that "*the lessons learned from Olympic security operations, for any nation, can have a huge impact on national security. They should be preserved, absorbed, and further developed.*"

A whole of government approach: It can be defined as "*public service agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to a particular issue. Approaches can be formal and informal. They can focus on policy development, program management, and service delivery*" (Management Advisory Committee, 2004). Whole of government envisages increased coherence across government and agency responsibilities. Canada established a master to run V2010 and G8/G20 security and safety in the PCO. It is then and only then that we have observed a clear orientation toward a whole of government approach. It is only this body that mandate collective exercises and training across all agencies and departments. There is considerable evidence of substantial effectiveness when agencies are aligned according to the same intent and goals. Without proper leadership, a whole of government approach loses its purpose and momentum.

Knowledge management system (KMS): KMS would create a functional repository for all of these best practices and lessons learned. Moreover, a cross agencies and department KMS might become a starting point for planning, execution and assessment of major events. This KMS should be collaborative, functional, usable, flexible and evolutionary. Kumar (2005-2006) proposed that "*success of the next generation knowledge management systems will depend upon integration of not only data processes across inter-enterprise supply chains and value chains, but also integration of decision-making and actions across inter-enterprise boundaries.*"

6   Conclusion

Command and Control of major events safety and security is de facto different from classical military Command and Control even when considering coalition operations. Culture, mandate, legislative constraints, technical and human differences militate toward an innovative Command and Control construct for major events. It is true that most military related C2 teaching that were learned over time across the spectrum of force employment missions have contributed to C2 of major events. The fundamental C2 theories and lessons observed have been used and exploited for V2010, G8 and G20 events. In this regard, the DRDC S&T community played a major role in the translation of those teaching and lessons for consumption (exploitation) by civilian (public and private) agencies and organizations.

In major events, it has been clearly established that C2 was the integrative layer of all safety and security operations. It is where operations are planned, coordinated, executed, adjusted and sustained. Proper training and exercising campaign plan supported by an engaged scientific methodology have been the most critical factor for the success of V2010 safety and security C2 construct and arrangements.

In this paper we presented the main C2 related concepts related major events. We discussed the Canadian experience of the S&T community in support of major events safety and security (i.e., V2010 and G8/G20). A full range of S&T activities have been planned and executed before and during these major events. The S&T community played a major role reducing the risk related to all aspect of safety and security operations. In particular, the S&T community helped shaping the C2 arrangements and solutions.

This paper proposed a set of lessons observed and recommendations to enable future major events C2 solutions based on the Canadian experience with V2010 and G8/G20 events.

7   References

Bellavita, C. (2002). The 2002 Olympic Winter Games Security Lessons Applied to Homeland Security. Salt Lake City: The Oquirrh Institute.

Caudle, S. L. (2005). Homeland Security Capabilities-Based Planning: Lessons from the Defense Community. Homeland Security Affairs .

Conners, E. (2004). Planning and Managing Security For Major Special Events. Washington: U.S. Department of Justice: Office of Community Oriented Policing Services.

FEMA (2006), U.S. Department of Homeland Security.(2006). NIMS and use of Plain Language. National Incident Management System. Washington: FEMA Publications.

FEMA (2008), U.S. Department of Homeland Security (2008) National Incident Management System. Washington: FEMA Publications.

FEMA. (2009). Developing and Maintaining State, Territorial, Tribal, and Local Government Emergency Plans. Washington: U.S. Department of Homeland Security.

Ford, R; Zuzzman D. (1997) Institutes of Public Administration Canada. Alternative Service Delivery: Sharing Governments in Canada.

French, S. P; Disher, E. (1997). Atlanta and the Olympics: A One-Year Retrospective. APA Journal.

Furst, P. (2009) Gis and Security. GiS Professional, 27, 9-12.

Huxham, C. (1991). Facilitating Collaboration: Issues in Multi-Organizational Group Decision Support in Voluntary, Informal Collaborative Settings. The Journal of the Operational Research Society , 1037-1045.

JCDS 21 (2008), Contractor Report on Characterisation of Complex Situation: JSTAFF Business Processes and the Canadian Incident Response Environment.

Johnson, C. W. (2006a). A Brief Overview of Technical and Organizational Security at Olympic Events. Glasgow: University of Glasgow.

Johnson, C.W. (2006b). On the Convergence of Physical and Digital Security for Public Safety at Olympic Events. Glasgow: University of Glasgow

Johnson, C.W. (2006c). Using Evacuation Simulations to Ensure the Safety and Security of the 2012 Olympic Venues. Glasgow: University of Glasgow

Kernaghan, K. (2009). IATF Governance Workshop. ISD Governance Considerations. St. Catherines: Brock University.

Kumar, S; Thondikulam, G. (2005-2006) Knowledge Management in a collaborative business framework. Information Knowledge Systems Management Vol. 5, Issue 3. 171-187

Management Advisory Committee (2004). Connecting Government – Whole of Government Responses to Australia's Priority Challenges. Canberra: Commonwealth of Australia, Copyright Administration.

Pourian, I., Everett, L., Cornester, J., Knudtson, P., Corwin, V. (2009), New Thinking on Major Event Safety and Security: Proposed New Strategic Management Framework, DRDC Contractor Report .

Pue, W., & Nemetz, N. (2009, April 07). Security for the Olympics: British Columbia Needs a "Public Order Policing Act". Vancouver, BC, Canada

Royal Canadian Mounted Police. (2009). RCMP Protective Policing Major Events. Vancouver, B.C., Canada.

Sotoodeh, M. (2007). Ontology Based Semantic Interoperability. Vancouver: University of British Columbia.

Thompson , D. (2008) Olympic Security Collaboration. China Security Vol. 4, No. 2, 46-58.

U.S. Department of Homeland Security (2008) National Incident Management System. Washington: FEMA Publications

U.S. Department of Homeland Security. (2009). The Integrated Planning System. Washington: U.S. Government.

U.S. Department of Homeland Security.(2006). NIMS and use of Plain Language. National Incident Management System. Washington: FEMA Publications.

U.S. Government Accountability Office. (2006). Olympic Security Better Planning Can Enhance U.S. Support to Future Olympic Games. Washington, D.C.

United States Government Accountability Office, Report on Olympic Security, June 30, 2006.

US Department of Justice Office of Community Oriented Policing Services (COPS), Major Events Security Guidelines.

Vancouver 2010 Integrated Security Unit. (2009, 04 16). 2010 ISU - Private Security Contract Announcement . Retrieved 05 30, 2009, from www.v2010isu.com: http://cb.grc.ca/ViewPage.action?siteNodeId=511&contentId=9157&index=3&languageId=1

Wildsmith J; Bradfield M. (2007). Halifax Commonwealth Games Bid: Were the Costs and Benefits Assessed? Canadian Centre for Policy Alternatives: Canada

Wilkins, J. (2003). Conceptual and Practical Considerations in Alternative Service Delivery. International Review of Administrative Sciences.

Wood, D. J., Gray, B. (1991). Toward a Comprehensive Theory of Collaboration. Arlington: Sage Publications.

Wood, D., Murray, C., Chouinard, P., Genik, L., Masys, T., Dixson, T., Dooley, P., Guitouni, A., MacLatchy, J., Major Events Coordinated Security Solutions: The Application of Science and Technology to reduce Risk for the Vancouver V2010 Winter Olympics and Paralympics and the G8/G20 Summits, DRDC CSS TR 2010-13.

Agenda

- Major Events Coordinated Security Solutions (MECSS) Project
- C2 Complexity
- C2 Domain of work
- Best Practices
- Conclusion

MECSS Objectives

- <u>Primary</u>:
  - Assist the functional authorities in **reducing the security risk associated with V2010** through the coordinated application of Science and Technology.

- <u>Secondary</u>:
  - Contribute to the establishment of an **enduring Major Event security architecture** that can be applied to future Major Events in Canada.

  Managed as a project under the Public Security Technical Program within Defence Research and Development Canada Centre for Security Science

MECSS Capability Domains
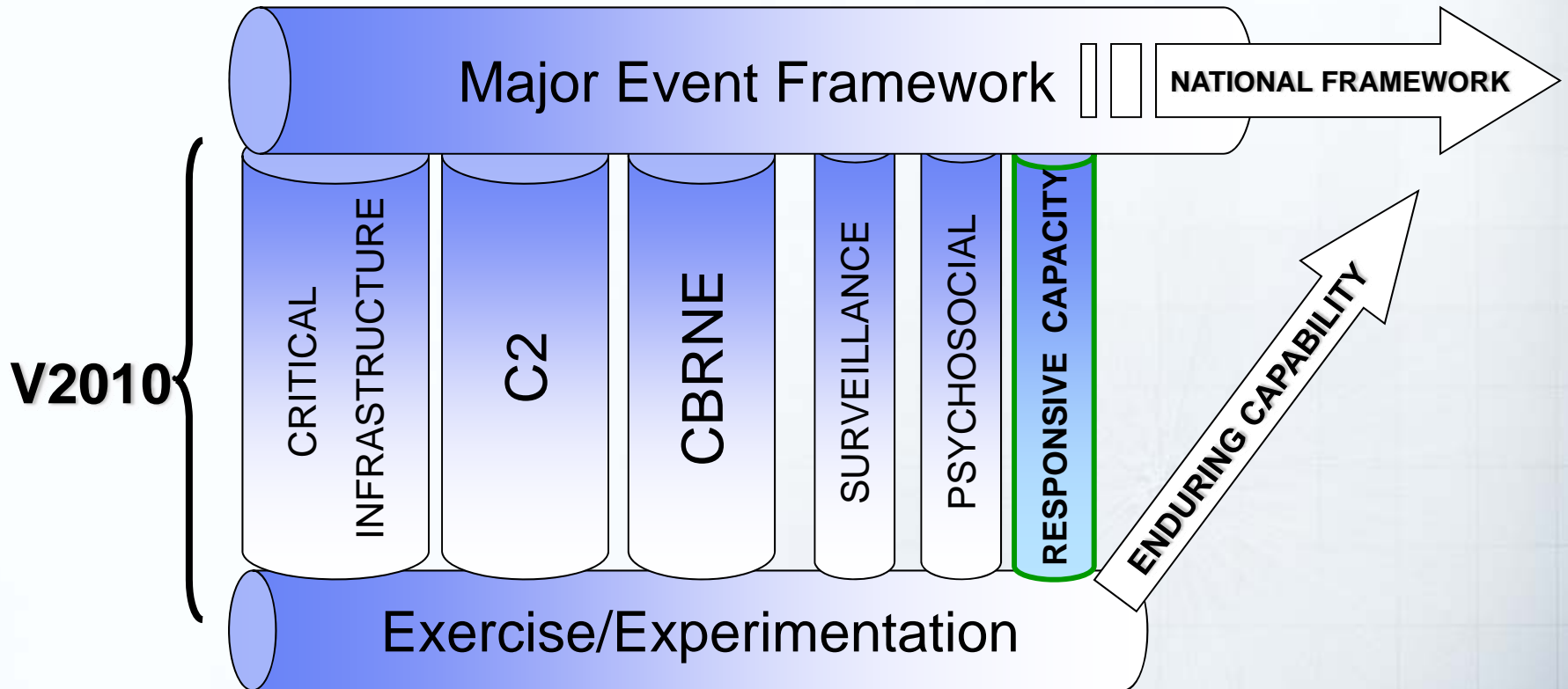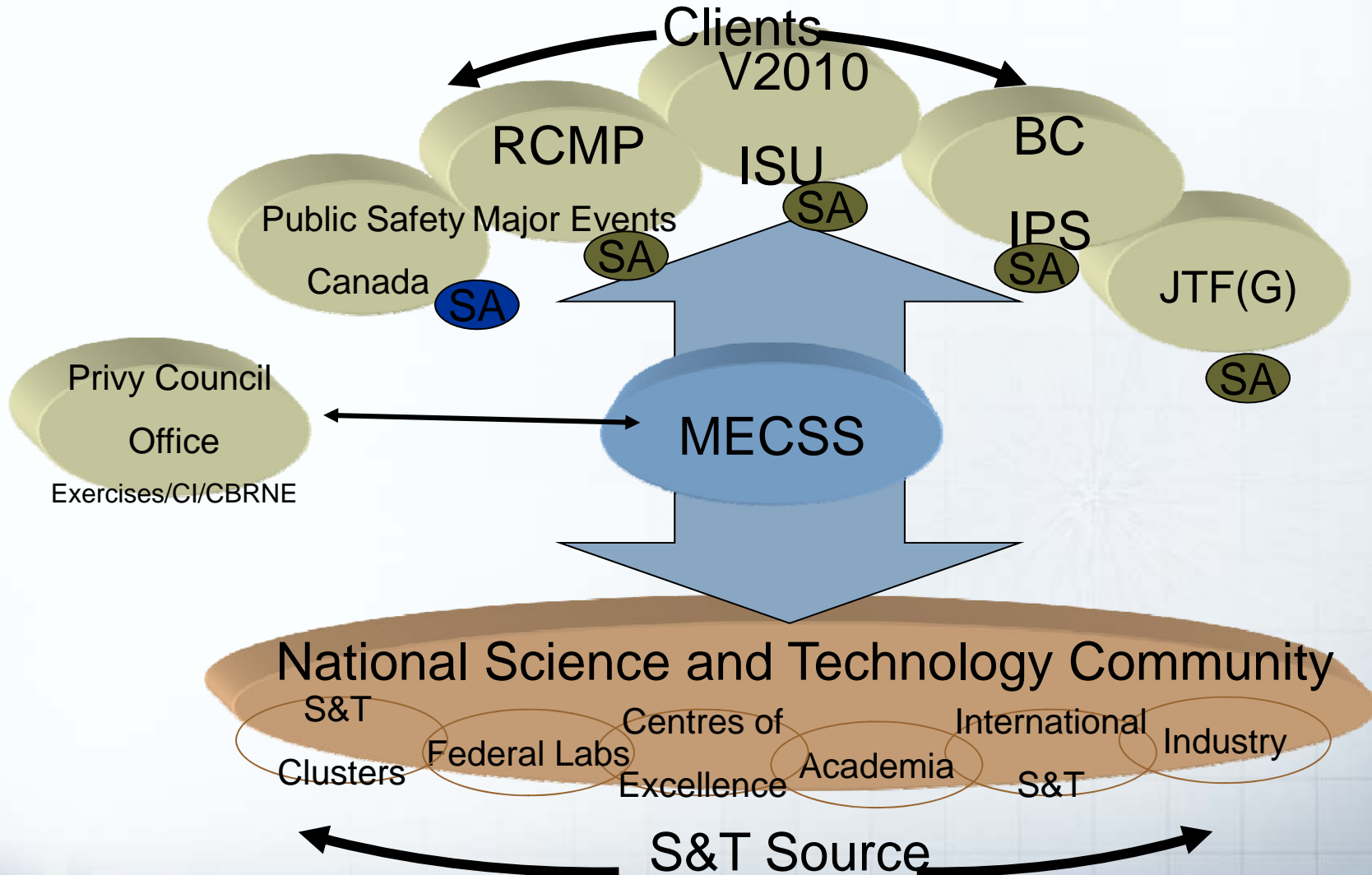
Variables Influencing Complexity of Response
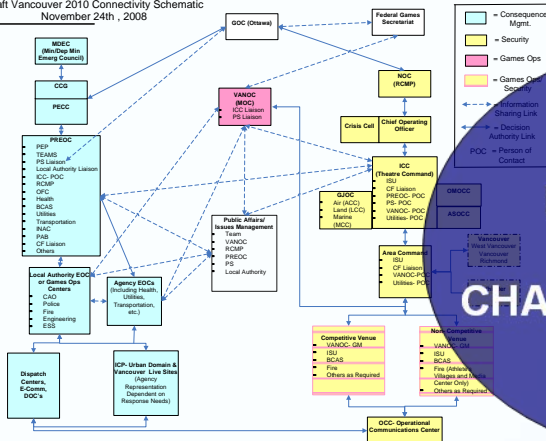
RESPONSE TEAM CHARACTERISTICS

ADVERSARY CHARACTERISTICS

COMPLEX SITUATION

ENVIRONMENT CHARACTERISTICS

INCIDENT CHARACTERISTICS
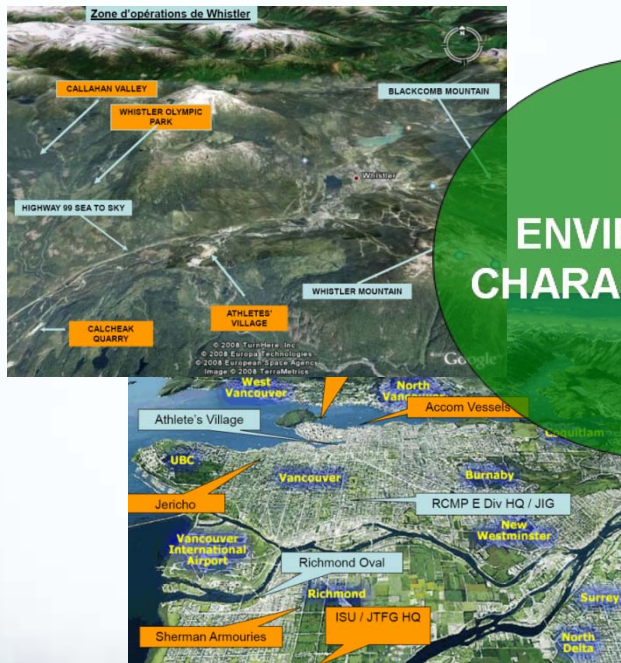
C2 Complexity of V2010

- Largest domestic security event in Canadian history
- Geography
  - 2.1M people in the Greater Vancouver area
  - 2 areas of operations – 150 sq km (Vancouver and Whistler)
  - Canada's busiest port/airspace
  - 30+ Olympic venues
- Organizations
  - 140 + federal/provincial/municipal organizations
- People
  - 5500 athletes and officials
  - 10,000 media
  - 25,000 Games volunteers
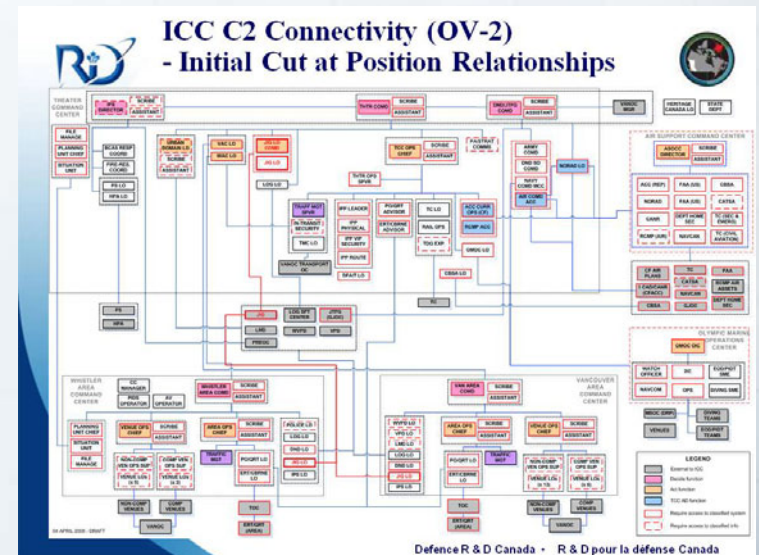 - 15,000 security workforce
- Event
  - 60 days of celebration
  - 27 days of sport
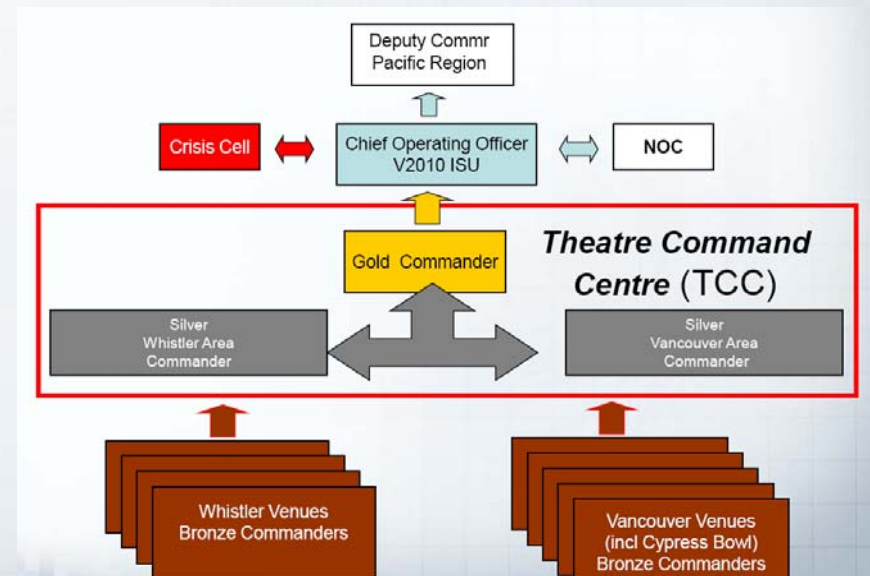
MECSS Activities in the C2 Domain (1/2)

- IT Architecture Options Analysis
- V2010 Integrated Security Unit C2 Concept of Operations
- Command Centre Designs
- C2 Architecture and Process Modeling
- Confirmation Architecture Framework

MECSS Activities in the C2 Domain (2/2)
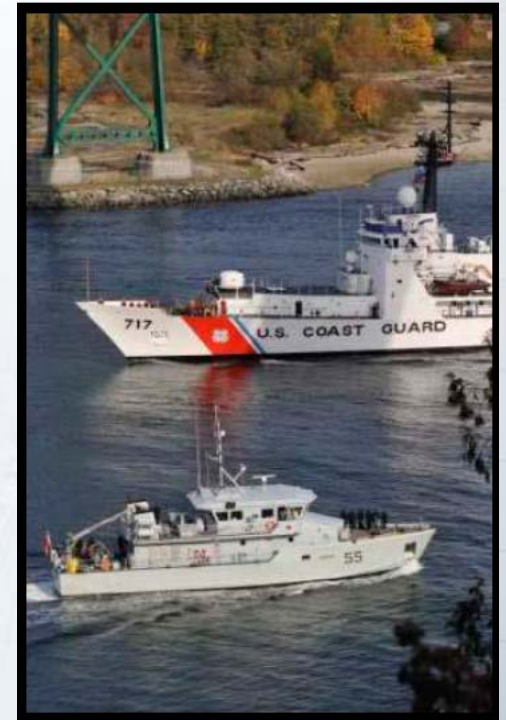
- Collaboration Framework
- Communication and Information System Studies
- Olympic Marine Operation Centre Analysis
- Shift Scheduling and Mobilization Planning
- Scientific Support to C2 Related Exercises
- Deployment of C4ISR Mobile Lab

Best Practices: Fostering Multi-Agency Collaborations

- Lead Agency
- Legal Authorities
- Perform Collaboration Situation Assessments

Best Practices: Collective Planning and Execution of Operations

- Pre-Event Planning
- Organizational Framework
- Leadership Structure
- C2 Centers and Infrastructures
- Assessment Model
- Collective and Individual Training
- Communication
- In-Progress Reviews
- Partnership Management
- Intelligence
- C2 of CBRNE Ops
- Public Safety
- Public Affairs
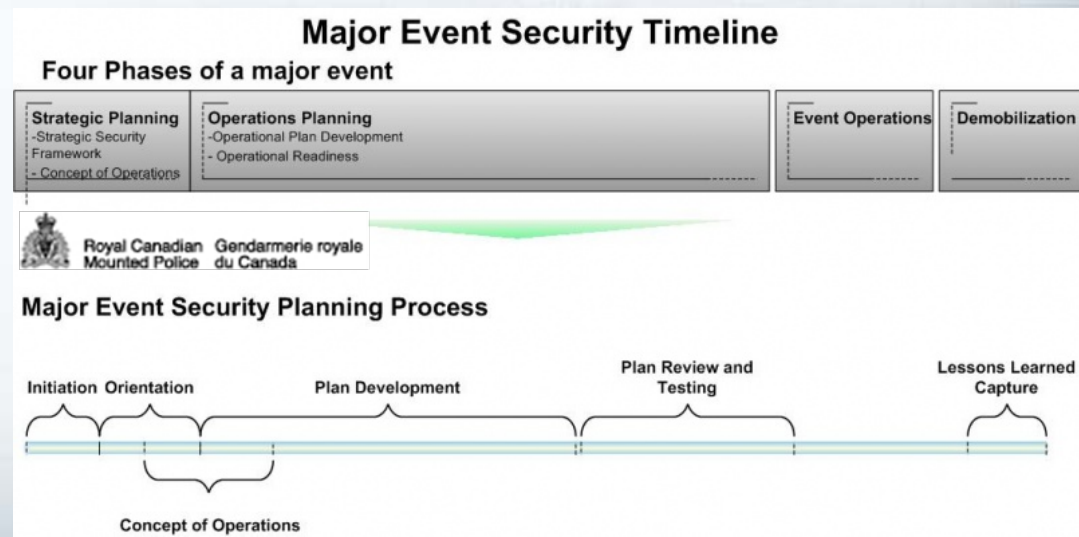- Private Sector Coordination

Best Practices: Potential Obstacles

- Limited Information Sharing
- Interoperability Issues
- Lack of Common Terminology
- Structure Silos
- Financial and Time Constraints
- Cultural Barriers
- Governance Issues

Potential Enablers

- Integrated Command Structures
- Common Information Sharing Systems and Protocols
- Outcome Management and Cost Reduction
- Scalable Governance Structures
- Community of Interests
- Whole of Government Approach
- Knowledge Management Systems

Major Event Security Timeline

Four Phases of a major event

Strategic Planning	Operations Planning	Event Operations	Demobilization
-Strategic Security Framework	-Operational Plan Development		
- Concept of Operations	- Operational Readiness		

Royal Canadian Gendarmerie royale
Mounted Police du Canada

Major Event Security Planning Process

Initiation Orientation — Plan Development — Plan Review and Testing — Lessons Learned Capture

Concept of Operations

Conclusion

- Complexity of C2 for major events requires a collaborative response from a large variety of stakeholders
- C2 is the integrative layer for major events safety and security operations
- Obstacles related to governance, culture, interoperability, terminology, etc are not trivial
- Integrated command structures, information sharing, whole of government approach, KMS, integrated planning framework are potential enablers

DEFENCE **R&D** DÉFENSE